McAfee VirusScan Enterprise 8.7i Product Guide

McAfee®

COPYRIGHT

Copyright © 2008 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Introducing VirusScan Enterprise **6**

Using VirusScan Enterprise 6

Getting started 8

What to do first 8

Where to find product information 9

Controlling Access to the User Interface **11**

How setting a password affects users 11

Configuring user interface security settings 11

Protecting Your System Access Points **13**

How access protection rules are defined 13

Access point violations and how VirusScan Enterprise responds 14

Types of user-defined rules 15

Configuring access protection settings 15

Configuring anti-virus and common rules 16

Configuring user-defined rules 16

Configuring port blocking rules 16

Configuring file/folder blocking rules 17

Configuring registry blocking rules 17

Including or excluding specific processes 18

Removing user-defined rules 18

Blocking Buffer Overflow Exploits **19**

How buffer overflow exploits are defined 19

Configuring buffer overflow protection 19

Restricting Potentially Unwanted Programs **21**

How potentially unwanted programs are defined 21

Configuring the unwanted programs policy 21

Updating Detection Definitions **23**

How an update strategy is determined 23

Update tasks and how they work 24

Configuring the AutoUpdate task 25

Mirror tasks and how they work. . . . 26
Configuring the mirror task. . . . 26
How the AutoUpdate repository works. . . . 26
Configuring the repository list. . . . 27
How rolling back DAT files works. . . . 27
Rolling back DAT files. . . . 27
Scanning Items On-Access. . . . 29
On-access scanning and how it works. . . . 29
Scanning comparison: writing to disk vs. reading from disk. . . . 30
Scanning comparison: scanning all files vs. scanning default + additional file types. . . . 30
Script scanning and how it works. . . . 30
Determining the number of scanning policies. . . . 31
Determining which risk to assign to a process. . . . 31
How general and process settings are configured. . . . 32
Configuring general settings. . . . 32
Configuring process settings. . . . 33
Scanning Items On-Demand. . . . 35
On-demand scanning methods and how they are defined. . . . 35
How scanning of remote storage works. . . . 35
How scan deferral works. . . . 36
How heuristic network check for suspicious files works. . . . 36
How system utilization works. . . . 36
Configuring on-demand scan tasks. . . . 37
Scanning Email On-Delivery and On-Demand. . . . 39
How heuristic network check for suspicious files works. . . . 39
Configuring email scan properties. . . . 39
Defining the Quarantine Policy. . . . 41
Configuring the quarantine policy and restoring items. . . . 41
Configuring Alerts and Notifications. . . . 43
Configuring alerts. . . . 43
Accessing Queries and Dashboards. . . . 44
Responding to Detections. . . . 45
How actions are taken on detections. . . . 45
System access point violations. . . . 45
Buffer overflow detections. . . . 46
Unwanted program detections. . . . 46

On-access scan detections. . . . 47
On-demand scan detections. . . . 47
Email scan detections. . . . 48
Quarantined items. . . . 48
Supplemental Information. . . . 49
Accessing user interface options. . . . 49
VirusScan Console and how it works. . . . 49
Using right-click features. . . . 50
System tray icon and how it works. . . . 51
Start menu and how it works with VirusScan Enterprise. . . . 51
Command line and using it to configure VirusScan Enterprise. . . . 52
Adding and excluding scan items. . . . 52
Specifying scan items. . . . 52
Specifying exclusions. . . . 52
Using wildcards to specify scan items. . . . 52
Scheduling tasks. . . . 53
Configuring the task schedule. . . . 53
Configuring command-line options. . . . 53
Configuring on-demand scanning command-line options. . . . 53
Configuring update task command-line options. . . . 55
Connecting to remote systems. . . . 56
Accessing remote systems with VirusScan Enterprise installed. . . . 56
Submitting threat samples for analysis. . . . 56
Accessing the Avert Labs Threat Library. . . . 57
Troubleshooting. . . . 57
Repairing the product installation. . . . 57
Frequently asked questions. . . . 58

Introducing VirusScan Enterprise

VirusScan Enterprise offers easily scalable protection, fast performance, and mobile design to protect your environment from viruses, worms, and Trojan horses. It also protects your system from access point violations, exploited buffer overflows, and potentially unwanted code and programs. It detects threats, then takes the actions you configured to protect your environment. See the VirusScan Enterprise Release Notes for information about what's new in this release.

This guide describes how to configure and use VirusScan Enterprise.

You can configure VirusScan Enterprise as a standalone product or you can use ePolicy Orchestrator versions 3.6.1 and 4.0 to centrally manage and enforce VirusScan Enterprise policies, then use queries and dashboards to track activity and detections.

NOTE: This document addresses using ePolicy Orchestrator 4.0. For information about using either version of ePolicy Orchestrator, see its product documentation.

Contents

- Using VirusScan Enterprise
- Getting started
- What to do first
- Where to find product information

Using VirusScan Enterprise

Use the VirusScan Enterprise software to protect your environment from potential threats.

When installed, VirusScan Enterprise is configured to use the detection definition (DAT) file that was packaged with the product and provide general security for your environment. We recommend that you define the policies and needs of your environment and configure the product accordingly, then update the product's detection definitions before you begin using the product or deploy it to client computers.

Each VirusScan Enterprise component or feature plays a part in protecting your environment.

Prevention

Define your security needs to ensure that all of your data sources are protected, then develop an effective strategy to stop intrusions before they gain access to your environment. Configure these features to prevent intrusions:

- User Interface Security — Set display and password protection to control access to the user interface.
- Access Protection — Use access protection rules to protect your computer from undesirable behavior with respect to files, registry, and ports. If you installed the AntiSpyware Enterprise

Module, you have additional rules to protect you from potentially unwanted spyware-related threats.

- Buffer Overflow Protection — Prevent exploited buffer overflows from executing arbitrary code on your computer.
- Unwanted Program Protection — Eliminate potentially unwanted programs such as spyware and adware from your computer.

Detection

Develop an effective strategy to detect intrusions when they occur. Configure these features to detect threats:

- Update Task — Get automatic updates of detection definitions and scanning engine from the McAfee download website.
- On-Access Scanning — Detect potential threats from any possible source as files are read from or written to disk. If you installed the AntiSpyware Enterprise Module, you can also scan for potentially unwanted cookies in the cookies folder.
- On-Demand Scan Tasks — Detect potential threats using immediate and scheduled scan tasks. If you installed the AntiSpyware Enterprise Module, you can also scan for potentially unwanted cookies and spyware-related registry entries that were not previously cleaned.
- On-Delivery and On-Demand Email Scanning — Detect potential threats on Microsoft Outlook email clients using on-delivery scanning of messages, attachments, and public folders. Detect potential threats on Lotus Notes email clients when messages are accessed.
- Quarantine Manager Policy — Specify the quarantine location and the length of time to keep quarantined items. Restore quarantined items as necessary.

Notification

Alerts and Notifications — Configure alerts to notify you when detections occur.

Response

Use product log files, automatic actions, and other notification features to decide the best way to handle detections.

- Log files — Monitor product log files to view a history of detected items.
- Queries and Dashboards — Use ePolicy Orchestrator queries and dashboards to monitor scanning activity and detections.
- Actions — Configure features to take action on detections.

Supplemental Information

Refer to these topics for additional information:

- Accessing user interface options — Access the standalone version of the product in a number of ways.
- Adding and Excluding Scan Items — Fine-tune the list of file types scanned for each of the scanners.
- Scheduling tasks — Schedule on-demand scan, update, and mirror tasks to run at specific dates and times, or intervals.
- Configuring command-line options — Configure on-demand scan and update tasks from the command line.

- Connecting to remote system — Connect to remote systems with VirusScan Enterprise installed to perform actions such as modify and schedule scanning or update tasks or to enable and disable the on-access scanner.
- Submitting threat samples for analysis — Submit samples of undetected potential threats to Avert Labs through WebImmune.
- Accessing the Avert Labs Threat Library — Access the information in the Avert Labs Threat Library.
- Troubleshooting — Get information about how to repair the product installation and frequently asked questions.

Getting started

We assume that you have the necessary privileges to perform the steps described in this guide.

1. Get the VirusScan Enterprise 8.7i product files from the McAfee download site. These files may include the product installation files, the product package file, the report and help extension files, and the ePolicy Orchestrator migration tool. See the VirusScan Enterprise 8.7i Release Notes for installation and known issues.
2. For ePolicy Orchestrator, use the Check-In Wizard to add the product and report extension files and the product package file to the repository. If you are upgrading from a previous version of VirusScan Enterprise and want to preserve settings, run the ePolicy Orchestrator migration tool. See the ePolicy Orchestrator product documentation for details.
3. For VirusScan Enterprise standalone installation, see the Installation Guide for details about installing the product. If you are upgrading from a previous version of VirusScan Enterprise, the Installation Guide describes how to preserve settings.

What to do first

When installed, VirusScan Enterprise is configured to use the detection definitions that were packaged with the product and provide general security for your environment. We recommend that you get the latest detection definitions and customize the configuration to meet your requirements before you deploy the product to client systems.

Task

Take these actions immediately after installing the product.

1. **Set user interface security**. Configure the display and password options to prevent users from accessing specific components or the entire VirusScan Enterprise user interface. See *Controlling Access to the User Interface* for more information.
2. **Update detection definitions**. Perform an **Update Now** task to ensure that you have the most recent detection definitions. See *Updating Detection Definitions* for more information.
3. **Prevent intrusions**. Configure these features to prevent potential threats from accessing your systems:
   - **Access Protection**. Configure access protection rules to prevent unwanted changes to your computer and enable the option to prevent McAfee processes from being terminated. See *Protecting Your System Access Points* for more information.

- **Buffer Overflow Protection**. Enable buffer overflow detection and specify exclusions. See *Blocking Buffer Overflow Exploits* for more information.
- **Unwanted Programs Policy**. Configure the policy that the on-access, on-demand, and email scanners use to detect potentially unwanted programs. Select categories of unwanted program categories to detect from a predefined list, then define additional programs to detect or exclude. See *Restricting Potentially Unwanted Programs* for more information.

4 **Detect intrusions**. Configure these features to detect potential threats on your systems, then notify you and take action when detections occur:

- **AutoUpdate**. Configure update tasks to get the most current detection definitions, scanning engine, and product upgrades. See *Updating Detection Definitions* for more information.
- **On-Access Scanner**. Configure the scanner to detect and take action on potential threats as they are accessed in your environment. Enable scanning of unwanted programs. If you installed the AntiSpyware Enterprise Module, you can also scan for cookies in the cookies folder. See *Scanning Items On-Access* for more information.
- **On-Demand Scanner**. Configure scan tasks to detect and take action on potential threats in your environment. Enable scanning of unwanted programs. If you installed the AntiSpyware Enterprise Module, you can also scan for cookies in the cookies folder and potentially unwanted spyware-related registry entries that were not previously cleaned. See *Scanning Items On-Demand* for more information.
- **Email Scanners**. Configure the on-delivery and on-demand scanning of Microsoft Outlook and Lotus Notes email clients. Enable scanning of unwanted programs. See *Scanning Email On-Delivery and On-Demand* for more information.

5 Send alerts and quarantine threats. Configure these features to alert you when detections occur and manage quarantined items:

- **Alerts and Notifications**. Configure how and when you receive detection notifications and alerts. See *Configuring Alerts and Notifications* for more information.
- **Quarantine Manager Policy**. Configure the location of the quarantine folder and the number of days to keep quarantined items before automatically deleting them. See *Defining the Quarantine Policy* for more information.

Where to find product information

The product documentation is designed to provide you with the information you need during each phase of product implementation, from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledgebase available on McAfee ServicePortal.

Installation Phase	Setup Phase	Maintenance Phase
Before, during, and after installation. *Release Notes* • Known issues in the current release. • Issues resolved since the last release.	Getting up-and-running with the product. *Product Guide* and *Online Help* • Setting up and customizing the software for your environment. *Online Help*	Maintaining the software. *Online Help* • Maintaining the software. • Reference information. • All information found in the product guide.

Installation Phase	Setup Phase	Maintenance Phase
• Last-minute changes to the product or its documentation. *Installation Guide* • Preparing for, installing and deploying software in a production environment.	• Managing and deploying products through ePolicy Orchestrator. • Detailed information about options in the product.	*Knowledgebase* (knowledge.mcaf) • Release notes and documentation. • Supplemental product information. • Workarounds to known issues.

Finding release notes and documentation for McAfee enterprise products

1. Go to knowledge.mcafee.com and select **Product Documentation** under **Useful links**.
2. Select **<Product Name>** | **<Product Version>** and select the required document from the list of documents.

Accessing help topics from the product

To access help topics:

- From the ePolicy Orchestrator console, click **?**, then select VirusScan Enterprise 8.7i.

  For option definitions, click **?** on the policy or task tab.

- From the VirusScan Console, select **Help Topics** from the **Help** menu.

  NOTE: The first time you access **Help** after installing the product, you are asked if you want to download the Help file. Click **Yes** to download the Help file and install it in your installation directory.

  For option definitions, click **Help** on the feature properties tab.

Controlling Access to the User Interface

Setting security for the interface on client computers is an important part of protecting your environment. As an administrator, you can control the access users have to the VirusScan Enterprise interface. Specify a password to prevent users from accessing or changing selected features. You can also lock and unlock the user interface as necessary.

Contents

- How setting a password affects users
- Configuring user interface security settings

How setting a password affects users

Set a user interface password to deter users with malicious intent. When you password-protect the user interface on client computers, users are affected as follows:

- **Non-administrators** — *Users without administrator rights*. Non-administrators run all VirusScan Enterprise applications in read-only mode. They can view some configuration parameters, run saved scans, and run immediate scans and updates. They cannot change any configuration parameters, create, delete, or modify saved scan or update tasks.
- **Administrators** — *Users with administrator rights*. Administrators must type the password to access the protected tabs and controls in read/write mode. If a password is not provided for a protected item, they view it in read-only mode.

Configuring user interface security settings

To access the **User Interface** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **User Interface Policies** in the **Category** list.
- From the VirusScan Console, select **Tools | User Interface Options**.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Display Options	• Specify which system tray icon options users can view. • Allow connections to remote computers. • Configure the console language.

Tab	Description
Password Options	Specify password security for the entire system or selected items.

Protecting Your System Access Points

Access protection prevents unwanted changes to your computer by restricting access to specified ports, files, shares, registry keys, and registry values. It also protects McAfee processes by preventing users from stopping them. This protection is critical before and during outbreaks.

This feature uses predefined rules and categories and user-defined rules to specify which items can and cannot be accessed. Each rule can be configured to block and/or report access point violations when they occur. Predefined rules and categories are subject to content updates via the McAfee update sites.

NOTE: The access protection feature uses the on-access scanner to detect access point violations. The on-access scanner must be enabled for the access protection feature to detect attempts to access ports, files, shares, and registry keys and values.

Contents

- How access protection rules are defined
- Access point violations and how VirusScan Enterprise responds
- Types of user-defined rules
- Configuring access protection settings

How access protection rules are defined

Rules are separated into these types and provide these levels of protection.

Rule type descriptions

Rule type	Description
Anti-virus	These preconfigured rules protect your computer from common behaviors of malware threats. You can enable, disable, and change the configuration, but you cannot delete these rules. Two rule examples are: • Prevent disabling or changing of critical processes, remote creation or modification of executable files, hijacking of executable files, Windows Process spoofing, and mass mailing worms from sending mail. • Protect phone book files from password and email stealers. These protection levels apply to anti-virus rules: • **Standard Protection** • **Maximum Protection** • **Outbreak Control**
Common	These preconfigured rules prevent modification of commonly used files and settings. You can enable, disable, and change the configuration, but you cannot delete these rules.

Rule type	Description
	Three rule examples are: • Prevent modification of McAfee files and settings. • Protect Mozilla and Firefox files and settings, Internet Explorer settings, and network settings. • Prevent installation of Browser Helper Objects and automatically running programs from the Temp folder. These protection levels apply to common rules. • **Standard Protection** • **Maximum Protection**
Virtual Machine Protection	These preconfigured rules prevent termination of VMWare processes and modification of VMWare files. You can enable, disable, and change the configuration, but you cannot delete these rules. Rule examples are: • Prevent termination of VMWAre Processes. • Prevent modification of VMWare workstation, server, or virtual machine files.
User-defined	These custom rules supplement the protection provided by the **Anti-virus** and **Common** rules.
Anti-spyware	If you installed the AntiSpyware Enterprise Module, you have additional rules to protect you from spyware-related threats. Rule examples are: • Prevent Internet Explorer favorites and settings. • Prevent programs from running and execution of scripts from the Temp folder.

Protection level descriptions

Protection Level	Description
Standard	Anti-virus and common rules that protect some critical settings and files from being modified, but generally allow you to install and execute legitimate software.
Maximum	Anti-virus and common rules that protect most critical settings and files from being modified. This level provides more protection than Standard, but might prevent you from installing legitimate software. If you cannot install software, we recommend that you disable the **Access Protection** feature first, then enable it again after installation.
Outbreak control	Anti-virus rules that block destructive code from accessing the computer until a DAT file is released. These rules are preconfigured to block access to shares during an outbreak.

Access point violations and how VirusScan Enterprise responds

When an access point violations occur:

- Information is recorded in the log file if you selected the **Report** option for the rule that detected the violation.

- The event is recorded in the local event log and to SNMP, if you configured **Alert Properties** to do so.
- The event is reported to Alert Manager and/or ePolicy Orchestrator, if those products are configured to do so.
- The **Block** and/or **Report** action is taken depending on which actions are configured for the rule that detected the violation.
- On the client system, a red frame surrounds the system tray icon and remains visible for 30 minutes unless you reset it.

  NOTE: To reset the icon, open the **Access Protection Log File** from the system tray icon. Opening the log file by any other method does not reset the icon to its normal state.

Types of user-defined rules

Choose from these three types of rules.

Rule descriptions

Rule	Description
Port Blocking Rule	Blocks incoming or outgoing network traffic on specific ports or ranges of ports. NOTE: When you block a port, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) accesses are blocked.
File/Folder Blocking Rule	Blocks read or write access to files and folders. NOTE: Once you restrict access to a file or folder, the restriction remains in place until the administrator removes it. This helps prevent intrusions and stops them from spreading during an outbreak.
Registry Blocking Rule	Protects registry keys or values by blocking these actions: read from, write to, create, or delete.

Configuring access protection settings

To access the **Access Protection** properties

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **Access Protection Policies** in the **Category** list.
- From the VirusScan Console, open the **Access Protection** properties.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Access Protection	• Enable access protection. • Configure rules. • Prevent McAfee processes from being stopped.

Tab	Description
Reports	• Enable activity logging. • Specify the log file name and location. • Specify the log file size limit. • Select the log file format.

Configuring anti-virus and common rules

Use predefined **Anti-virus** and/or **Common** rules to protect your computer from unwanted changes. These rules can be enabled and edited, but they cannot be deleted.

Task

1. Select the **Anti-virus** or **Common** category in the left pane, then select the specific rule in the right pane.
2. Configure the **Block** and/or **Report** options.
3. Click **Edit** to configure **Rule Details**.

Configuring user-defined rules

Create and edit user-defined rules to supplement the protection provided by the **Anti-virus** and **Common** rules.

Task

1. Select the **User-defined Rules** category in the left pane, then click **New**.
2. Select the rule type.
3. Change the **Block** and **Report** actions as necessary.
4. Click **Edit** to change the configuration.

Configuring port blocking rules

Block users from accessing specified inbound and/or outbound ports.

Option definitions

Option	Definition
Rule Name	Type the name for this rule.
Processes to include	Restrict access to the specified processes.
Processes to exclude	Allow access to the specified processes.
Starting Port	Specify the first port number. This can be a single port or the starting number of a range of ports. NOTE: If you block access to a port that is used by the McAfee Agent, the Entercept Agent, or the Host Intrusion Prevention Agent, the agent's processes are trusted and are allowed to communicate with the blocked port. All other traffic not related to these agent processes is blocked.
Ending Port	Specify the last port number in a range of ports.

Option	Definition
Inbound	Prevent systems on the network from accessing the specified ports.
Outbound	Prevent local processes from accessing the specified ports on the network.

Configuring file/folder blocking rules

Prevent users from taking action on specified files or folders.

Option definitions

Option	Definition
Rule name	Type the name for this rule.
Processes to include	Restrict access to the specified processes.
Processes to exclude	Allow access to the specified processes.
File or folder name to block	Block access to the specified file or folder.
Browse file	Navigate to the file.
Browse folder	Navigate to the folder.
Read access to files	Block read access to the specified files.
Write access to files	Block write access to the specified files.
Files being executed	Block files from being executed in the specified folder.
New files being created	Block new files from being created in the specified folder.
Files being deleted	Block files from being deleted from the specified folder.

Configuring registry blocking rules

Block users from taking action on specified registry keys or values.

Option definitions

Option	Definition
Rule Name	Specify the name for this rule.
Processes to include	Restrict access to the specified processes.
Processes to exclude	Allow access to the specified processes.
Registry key or value to protect	Protect this registry key or value: • Select a root key or value from the drop-down list. • Type a key or value in the text box. Selecting the root key or value from the drop-down list is optional. Use either of these methods to specify the key or value: • Select the root key or value from the drop-down list, then type the remaining path to the key or value in the text box. • Type the full path to the key or value in the text box.

Option	Definition
Rule type	Select the type of rule: • **Key** — This rule protects the specified key. • **Value** — This rule protects the specified value.
Write to key or value	Block writing to the specified key or value.
Create key or value	Block creating the specified key or value.
Delete key or value	Block deleting the specified key or value.

Including or excluding specific processes

Edit the rule details to specify processes that you want to detect or exclude from detection.

Option definitions

Option	Description
Rule Name	The name of this rule. For example, **Prevent registry editor and Task Manager from being disabled**.
Processes to include	Restrict access to these processes. Use the exact process name or use a wildcard to specify a broad range of processes such as *.EXE, then add exclusions for specific processes that are legitimate, such as SETUP.EXE. For example, specify * to include all processes.
Processes to exclude	Allow access to these processes. Use the exact process name. For example, specify these exclusions: avtask.exe, cfgwiz,exe, fssm32.exe, giantantispywar*, kavsvc.exe, mmc.exe, navw32.exe, nmain.exe, rtvscan.exe.

Removing user-defined rules

Remove rules that you created but no longer use.

Task

1 Select the **User-defined Rules** category in the left pane, then select the rule you want to remove in the right pane.

2 Click **Delete**.

NOTE: To disable a rule without deleting it, deselect the **Block** and **Report** actions. You can enable the rule again if necessary.

Blocking Buffer Overflow Exploits

Buffer overflow protection prevents exploited buffer overflows from executing arbitrary code on your computer. It monitors user-mode API calls and recognizes when they are called as a result of a buffer overflow.

When a detection occurs, information is recorded in the activity log and displayed in the **On-Access Scan Messages** dialog box if you configured those options to do so.

VirusScan Enterprise uses a Buffer Overflow and Access Protection DAT file to protect approximately 20 applications, including Internet Explorer, Microsoft Outlook, Outlook Express, Microsoft Word, and MSN Messenger.

Contents

- How buffer overflow exploits are defined
- Configuring buffer overflow protection

How buffer overflow exploits are defined

A buffer overflow exploit is an attack technique that exploits a software design defect in an application or process to force it to execute code on the computer. Applications have fixed-size buffers that hold data. If an attacker sends too much data or code into one of these buffers, the buffer overflows. The computer then executes the code that overflowed as a program. Since the code execution occurs in the security content of the application, which is often at a highly-privileged or administrative level, intruders gain access to execute commands not usually accessible to them. An attacker can use this vulnerability to execute custom hacking code on the computer and compromise its security and data integrity.

Configuring buffer overflow protection

To access the **Buffer Overflow Protection** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **Buffer Overflow Protection Policies** in the **Category** list.
- From the VirusScan Console, open the **Buffer Overflow Protection** properties.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Buffer Overflow Protection	• Enable buffer overflow protection. • Configure the detection mode to warn and/or protect you from buffer overflows. • Display the **On-Access Scan Messages** dialog box when a detection occurs.
Reports	• Enable activity logging. • Specify the log file name and location. • Specify the log file size limit. • Select the log file format.

Restricting Potentially Unwanted Programs

VirusScan Enterprise protects your computer from potentially unwanted programs that are a nuisance or present a security risk. One common unwanted program policy is configured, but you can individually enable or disable the policy and specify actions for each of the VirusScan Enterprise scanners.

Contents

- How potentially unwanted programs are defined
- Configuring the unwanted programs policy

How potentially unwanted programs are defined

Potentially unwanted programs are defined as software programs written by legitimate companies that can alter the security state or the privacy policy of the computer on which they are installed. This software can but does not necessarily include spyware, adware, and dialers. These programs can be downloaded with a program that the user wants. Security-minded users recognize such programs and, in some cases, remove them.

Configuring the unwanted programs policy

Configuration is a two-step process:

1. Define which potentially unwanted programs to detect and exclude:
   - Select whole categories of programs or specific programs within a category from a predefined list which comes from the current DAT file.
   - Specify exclusions.
   - Create a list of user-defined programs to detect.
2. After configuring the **Unwanted Programs Policy**, enable unwanted program detection in the on-access, on-demand, and email scanners, then configure which actions to take when an unwanted program is detected.

To access the **Unwanted Programs** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **Unwanted Programs Policies** in the **Category** list.
- From the VirusScan Console, open the **Unwanted Programs Policy** properties.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Scan Items	• Select the categories of unwanted programs to detect. For example, spyware, adware, etc. These categories are defined by the current DAT file. • Specify exclusions.
User-Defined Items	Define additional unwanted programs for detection.

Updating Detection Definitions

VirusScan Enterprise software depends on the scanning engine and the information in the detection definition (DAT) files to identify and take action on threats. New threats appear on a regular basis. To meet this challenge, McAfee releases new DAT files every day, incorporating the results of its ongoing research. The update task retrieves the most current DAT files, EXTRA.DAT file, scanning engine, Service Packs, and Patches.

Contents

- How an update strategy is determined
- Update tasks and how they work
- Mirror tasks and how they work
- How the AutoUpdate repository works
- How rolling back DAT files works

How an update strategy is determined

Updates can be accomplished using many methods. You can use update tasks, manual updates, login scripts, or schedule updates with management tools. This section describes using the update task. Any other methods are beyond the scope of this guide.

An efficient updating strategy generally requires that at least one client or server in your organization retrieve updates from the McAfee download site. From there, the files can be replicated throughout your organization, providing access for all other computers. Ideally, you should minimize the amount of data transferred across your network by automating the process of copying the updated files to your share sites.

The main factors to consider for efficient updating are the number of clients and the number of sites. You might also consider the number of systems at each remote site and how remote sites access the Internet. However, the basic concepts of using a central repository to retrieve updates and scheduling update tasks to keep your environment up-to-date apply to any size organization.

Using an update task allows you to:

- Schedule network-wide DAT file rollouts at convenient times and with minimal intervention from either administrators or network users. You might, for example, stagger your update tasks, or set a schedule that phases in, or rotates, DAT file updates to different parts of the network.
- Split duties for rollout administration among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the waiting time required to download new DAT or upgraded engine files. Traffic on McAfee computers increases dramatically on regular DAT file publishing dates and

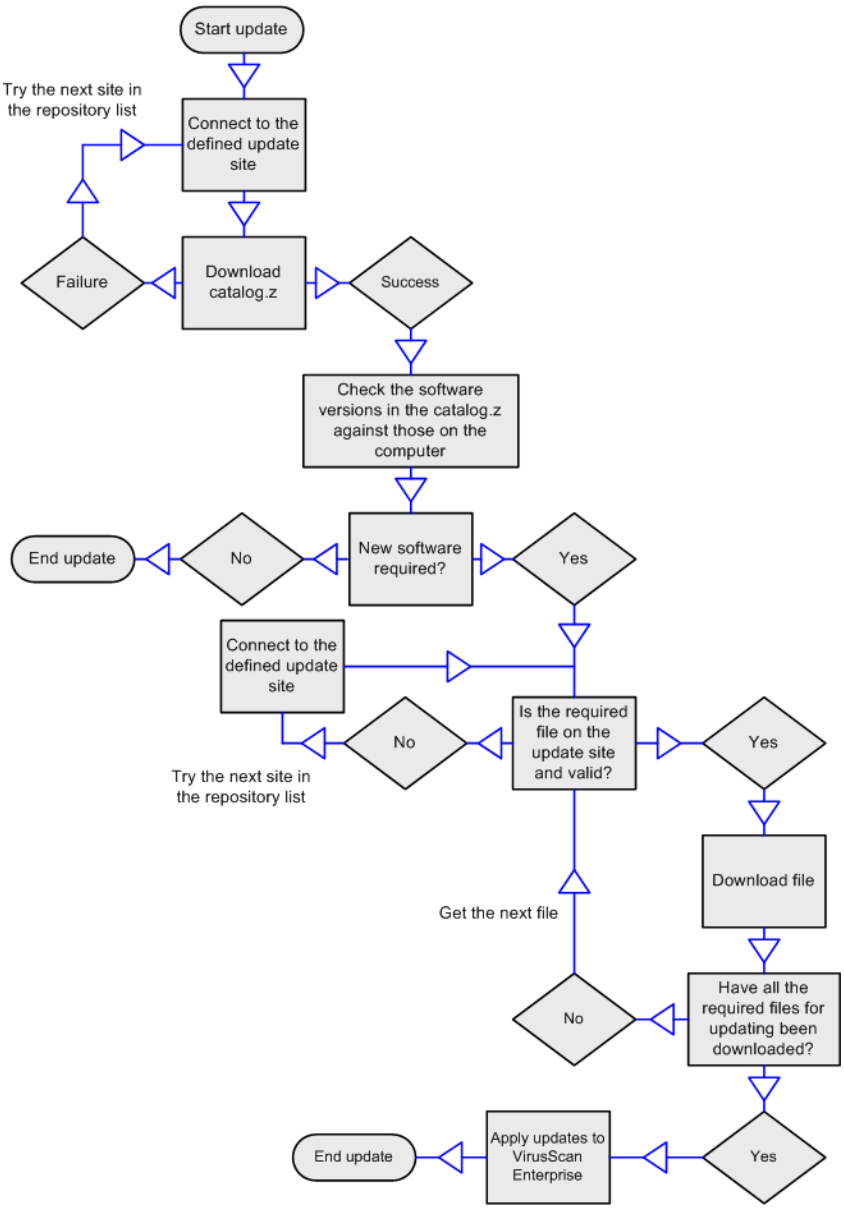
whenever new product versions are available. Avoiding the competition for network bandwidth enables you to deploy your new software with minimal interruptions.

Update tasks and how they work

Use the update task to get the most current DAT files, scanning engine, and Service Packs and Patches.

VirusScan Enterprise includes a default update task. The default task is scheduled to update every day at 5:00 p.m. with one-hour randomization. You can also create additional update tasks to meet your updating requirements.

This diagram shows how a typical update task works:



Update task activities

These activities occur when you run an update task:

- A connection is made to the first *enabled* repository (update site) in the repository list. If this repository is not available, the next site is contacted, and so on until a connection is made, or until the end of the list is reached.
- An encrypted CATALOG.Z file downloads from the repository. The file contains the fundamental data required to update. This data is used to determine which files and/or updates are available.
- The software versions in the file are checked against the versions on the computer. If new software updates are available, they are downloaded.
- Once the update is checked in to the repository, the update is verified to confirm that it is applicable to VirusScan Enterprise and that the version is newer than the current version. Once this is verified, VirusScan Enterprise downloads the update when the next update task runs.

Update task interruption

If the update task is interrupted for any reason during the update:

- A task updating from an HTTP, UNC, or local site resumes where it left off the next time the update task starts.
- A task updating from an FTP site does not resume if interrupted during a single file download. However, if the task is downloading several files and is interrupted, the task resumes before the file that was being downloaded at the time of the interruption.

Update using EXTRA.DAT

An EXTRA.DAT file can be used as a temporary measure in an emergency. The EXTRA.DAT is downloaded from the repository on each update. This ensures that if you modify and re-check in the EXTRA.DAT in as a package, all VirusScan Enterprise clients download and use the same updated EXTRA.DAT package. For example, you may use the EXTRA.DAT as an improved detector for the same potentially unwanted program or additional detection for other new potentially unwanted programs. VirusScan Enterprise supports using only one EXTRA.DAT file.

TIP: When you have finished using the EXTRA.DAT file, you should remove it from the master repository and run a replication task to ensure it is removed from all distributed repository sites. This stops VirusScan Enterprise clients from attempting to download the EXTRA.DAT file during an update. By default, detection for the new potentially unwanted program in the EXTRA.DAT is ignored once the new detection definition is added to the daily DAT files.

Configuring the AutoUpdate task

To access the **AutoUpdate** properties:

- From the ePolicy Orchestrator console, go to **Systems | System tree | Client Task**. Select an existing update task or to create a new task, click **New Task** , then from the **Type** list, select **Update (McAfee Agent)** and click **Next**.
- From the VirusScan Console, select an existing update task or to create a new task, select **Task | New Update Task**.

Configure the options on the tab. For option descriptions, click **?** or **Help** on the tab.

Tab description

Tab	Description
Update	• Specify the log file location and format. • Configure whether to get newer detection definitions, newer engine and DATs, and other available updates such as service packs, and product upgrades.

Tab	Description
	• Specify which executable to run after the update task has completed and whether to run it only after a successful update.

Mirror tasks and how they work

The mirror task replicates the update files from the first accessible repository defined in the repository list, to a mirror site on your network. The most common use of this task is to mirror the contents of the McAfee download site to a local server.

The VirusScan Enterprise software relies on a directory structure to update itself. When mirroring a site, it is important to replicate the entire directory structure.

NOTE: This directory structure also supports previous versions of VirusScan and NetShield, as long as the entire directory structure is replicated in the same locations that VirusScan 4.5.1 used for updating.

After you replicate the McAfee site that contains the update files, computers on your network can download the files from the mirror site. This approach is *practical* because it allows you to update any computer on your network, whether or not it has Internet access; and *efficient* because your systems are communicating with a server that is probably closer than a McAfee Internet site, economizing access and download time.

Configuring the mirror task

To access the **Mirror** task properties:

- From the ePolicy Orchestrator console, go to **Systems | System tree | Client Task**. Select an existing mirror task or to create a new task, click **New Task** , then from the **Type** list, select **Mirror (McAfee Agent)** and click **Next**.
- From the VirusScan Console, select an existing mirror task or to create a new task, select **Task | New Mirror Task**.

Configure the options on the tab. For option descriptions, click **?** or **Help** on the tab.

Tab description

Tab	Description
Mirror	• Specify the log file location and format. • Specify which executable to run after the mirror task has completed and whether to run it only after a successful mirror.

How the AutoUpdate repository works

The AutoUpdate repository list (SITELIST.XML) specifies the configuration information necessary to perform an AutoUpdate task. For example:

- Repository information and location.
- Repository order preference.
- Proxy settings, where required.

- Encrypted credentials required to access each repository.

When an AutoUpdate task is performed, a connection is made to the first *enabled* repository (update site) in the repository list. If this repository is not available, the next repository is contacted, and so on until a connection is made, or until the end of the list is reached.

Proxy servers are used as part of the Internet security to hide Internet users' computers from the Internet and improve access speed by caching commonly accessed sites. If your network uses a proxy server, you can specify which proxy settings to use, the address of the proxy server, and whether to use authentication. Proxy information is stored in the AutoUpdate repository list. The proxy settings you configure apply to all repositories in the repository list.

The location of the AutoUpdate repository list depends on your operating system. For example, for Windows XP:

C:\Documents and Settings\All Users\Application Data\McAfee\Common Framework

Configuring the repository list

The repository list includes the repositories from which you retrieve updates. Create and configure as many repositories as you need. Some sites can be used all the time while others are used only occasionally.

To access the **AutoUpdate Repository List** properties:

- From the VirusScan Console, select **Tools | User Interface Options**.

NOTE: This feature is not available from the ePolicy Orchestrator console.

Configure the options on the tab. For option descriptions, click **Help** on the tab.

Tab descriptions

Tab	Description
Repositories	• Specify the repositories from which you get updates. • Configure the order in which the repositories are accessed.
Proxy settings	Specify which proxy settings to use when updating.

How rolling back DAT files works

If you find your current DAT files are corrupted or incompatible, you can roll back the DAT files to the last backed up version.

When you update DAT files, the old version is stored in this location: <drive>:\Program Files\Common Files\McAfee\Engine\OldDats. When you roll back the DAT files, the current DAT files are replaced with the version in the *OldDats* folder, and a flag is set in the registry at this location: HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\DesktopProtection\szRolledbackDATS. Once the roll back occurs, you cannot go back to the previous version again. The next time an update occurs, the DAT version in the registry is compared with the DAT files in the update repository. If the new DAT files are the same as those in the registry, no update occurs.

Rolling back DAT files

To roll back the DAT files to the previous version.

Task

1 From the VirusScan Console, select **Tools | Rollback DATs**.

2 Click **Yes** to proceed with the DAT roll back.

NOTE:

This feature is not available from the ePolicy Orchestrator console.

Configure the options on the tab. For option descriptions, click **Help** on the tab.

Scanning Items On-Access

The on-access scanner examines files on your computer as they are accessed to provide continuous, real-time detection of threats. Both the Access Protection and Buffer Overflow Protection features also use the on-access scanner to detect access point violations and buffer overflow exploits respectively.

Contents

- On-access scanning and how it works
- Script scanning and how it works
- Determining the number of scanning policies
- Determining which risk to assign to a process
- How general and process settings are configured
- Configuring general settings
- Configuring process settings

On-access scanning and how it works

The on-access scanner hooks into the system at the lowest levels (File-System Filter Driver), acts as part of the system (System Service), and delivers notifications via the interface when detections occur.

This example describes what happens when an attempt is made to open, close, or rename a file. The scanner intercepts the operation and takes these actions.

1 The scanner determines if the file should be scanned based on this criteria:
- The file's extension matches the configuration.
- The file has not been cached.
- The file has not been excluded.
- The file has not been previously scanned.

2 If the file meets the scanning criteria, it is scanned:
- If the file is clean, the result is cached and read, write, or rename operation is granted.
- If the file contains a threat, the operation is denied and the configured action is taken.
- The results are recorded in the activity log if the scanner was configured to do so.

3 If the file does not meet the scanning requirements, it is not scanned. It is cached and the operation is granted.

Scanning comparison: writing to disk vs. reading from disk

The on-access scanner treats scans differently depending on whether the user is writing to disk or reading from disk.

When files are being written to disk, it scans these items:

- Incoming files being written to the local hard drive.
- Files being created on the local hard drive or a mapped network drive (this includes new files, modified files, or files being copied or moved from one drive to another).

When files are being read from disk, it scans these items:

- Outgoing files being read from the local hard drive. Select **On network drives** on the **Scan Items** tab to include remote network files.
- Any file being executed on the local hard drive.
- Any file opened on the local hard drive.
- Any file being renamed on the local hard drive, if the file properties have changed.

Scanning comparison: scanning all files vs. scanning default + additional file types

The on-access scanner treats scans differently depending on whether it is configured to scan all files or to scan default plus additional file types.

When scanning **All files**, the scanner scans every file type for all possible threats.

When scanning **Default + additional file types**, the scanner examines a specific list of files based on the file types you select.

- **Default file types**: the scanner examines the specified file type only for threats that attack that file type. For example, when scanning an XLS file, the scanner scans XLS files for threats that attack XLS files, such as macros. The scanner does not scan the XLS files for threats like PE (portable executable) infectors or even the EICAR test file. If the XLS file is renamed to that different file type, the scanner scans the renamed file for the threats that affect the newly named file type.
- **Additional file types**: the scanner scans the file type for all possible threats, as it does for **All files**.

Script scanning and how it works

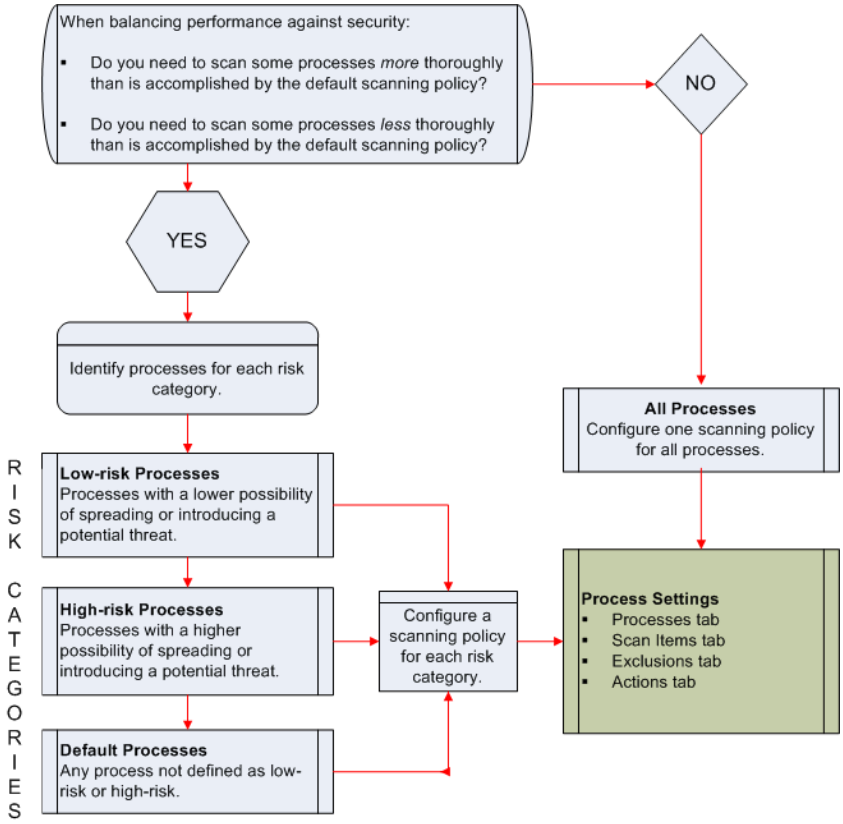
The script scanner operates as a proxy component to the real Windows scripting host component. It intercepts scripts, then scans them before they are executed.

- If the script is clean, it is passed on to the real scripting host component.
- If the script contains a potential threat, the script is not executed.

The script scanner loads into the process that's running the script, so if that process crashes, you see ScriptProxy.dll and Mytilus.dll in its memory space. It loads the DAT file and scan engine too, which significantly increases the memory footprint of that process.

Determining the number of scanning policies

Follow this process to determine whether to configure more than one on-access scanning policy:


When balancing performance against security:
Do you need to scan some processes more thoroughly than is accomplished by the default scanning policy?
Do you need to scan some processes less thoroughly than is accomplished by the default scanning policy?
NO
YES
Identify processes for each risk category.
All Processes
Configure one scanning policy for all processes.
RISK CATEGORIES
Low-risk Processes
Processes with a lower possibility of spreading or introducing a potential threat.
High-risk Processes
Processes with a higher possibility of spreading or introducing a potential threat.
Default Processes
Any process not defined as low-risk or high-risk.
Configure a scanning policy for each risk category.
Process Settings
Processes tab
Scan Items tab
Exclusions tab
Actions tab

Determining which risk to assign to a process

Once you decide that you need more than one scanning policy, identify your processes and determine which risk to assign to each one.

Task

1. Determine which processes you are using. Use the Windows Task Manager or Windows Performance Monitor to help you understand which processes are using the most CPU time and memory.
2. Determine which program is responsible for each process. Remember that only the child processes of the defined parent process adhere to the scanning policy. For example, if you define the Microsoft Word executable file, WINWORD.EXE, as a high-risk process, any Microsoft Word documents that are accessed would be scanned according to the high-risk scanning policy. However, when the parent process Microsoft Word is launched, the WINWORD.EXE file is scanned according to the policy of the process that launched it.
3. Determine which risk applies to each process using these guidelines:
   - **Low-risk** — Processes with less possibility of spreading or introducing a potential threat. These can be processes that access many files, but in a way that has a lower risk of spreading potential threats. For example:

Backup software

Compiling processes

- **High-risk** — Processes with a greater possibility of spreading or introducing a potential threat. For example:

  Processes that launch other processes, such as Microsoft Windows Explorer or the command prompt.

  Processes that execute scripts or macros, such as WINWORD or CSCRIPT.

  Processes used for downloading from the internet, such as browsers, instant messengers, or mail clients.

  NOTE: Initially, the high-risk scanning policy is set the same as the policy for default processes to ensure that high-risk processes are scanned in depth and give you the maximum protection. We do not recommend reducing the default level of scanning.

- **Default** — Any process not defined as low-risk or high-risk.

How general and process settings are configured

The on-access scanner's general and process policies are configured separately.

- **General Settings** — The general policy includes options that apply to all processes.
- **Process Settings** — The process settings allow you to configure one scanning policy for all processes or configure different policies for processes that you define as default, low-risk, and high-risk.

Configuring general settings

General settings apply to the scanning of all processes and include parameters such as maximum scan time, scanning scripts, blocking unwanted threats from a remote computer, sending messages when threats are detected, and reporting detections.

To access the **On-Access General** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **On-Access General Policies** in the **Category** list.
- From the VirusScan Console, open the **On-Access Scanner** properties, then select **General Settings** in the left pane.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
General	• Scan boot sectors and/or floppy drives during shutdown. • Enable on-access scanning at system startup. • Maximum scan time for archives and all files. • Scan all processes which are already running. • If the AntiSpyware Enterprise Module is installed, scan cookie files.

Tab	Description
ScriptScan	Enable scanning of scripts and specify exclusions.
Blocking	• Send a message when a remote computer writes a threat to this system and specify the message. • Block the connection when a remote computer writes a threat to this system. • Unblock the connection after the specified time. • Block the connection when a file with a potentially unwanted program is detected in a shared folder.
Messages	• Display the messages dialog box to local users when a detection occurs and specify the message. • If the AntiSpyware Enterprise Module is installed, send an alert when a cookie is detected. • Configure which actions users without administrator rights can take on messages.
Reports	• Enable activity logging. • Specify the log file name and location. • Specify the log file size limit. • Select the log file format. • Specify what to log besides scanning activity.

Configuring process settings

On-access scan processes are configured based on the risk that you assign to each process. You can configure one default scanning policy for all processes or configure different policies based on the risk assigned to each process. Parameters include assigning risk to processes, defining items to scan, performing heuristic scanning, scanning compressed files, taking actions on detections, and scanning for potentially unwanted programs.

To access the **Default Processes**, **Low-Risk Processes**, or **High-Risk Processes** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **On-Access Default Processes Policies**, **On-Access Low-Risk Processes Policies**, or **On-Access High-Risk Processes Policies** in the **Category** list.
- From the VirusScan Console, open the **On-Access Scanner** properties, then select **Default Processes**, **Low-Risk Processes**, or **High-Risk Processes** in the left pane.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Processes	• **On-Access Default Processes** — Choose to configure one scanning policy for all processes or configure different scanning policies for default processes, low-risk processes, and/or high-risk processes. NOTE: If you choose to configure one scanning policy, this policy applies to all processes. If you choose to configure different scanning policies for low-risk and/or high risk policies, this policy applies only to the processes that are not defined as low-risk or high-risk.

Tab	Description
	• **On-Access Low-Risk Processes** — Specify the processes that you define as low-risk. • **On-Access High-Risk Processes** — Specify the processes that you define as high-risk. NOTE: The **Configure different scanning policies for high-risk, low-risk, and default processes** option must be selected on the **On-Access Default Processes** tab before you can configure individual policies for low-risk and/or high-risk processes.
Scan Items	• Configure whether to scan files on read, on write, on network drives and/or opened for backup. • Configure which files and file types to scan. • Scan for potential threats that resemble unwanted programs, Trojan horses and macro viruses. • Scan inside archives and decode MIME encoded files. • Enable on-access scanning for unwanted programs.
Exclusions	Configure which disks, files, and folders to exclude from scanning.
Actions	For threat detections: • Primary action to take when a threat is detected. • Secondary action to take on a threat detection if the first action fails. For unwanted program detections: • Primary action to take when an unwanted program is detected. • Secondary action to take on an unwanted program detection if the first action fails.

Scanning Items On-Demand

The on-demand scanner provides a method for scanning all parts of your computer for potential threats, at convenient times or at regular intervals. Use on-demand scans to supplement the continuous protection that the on-access scanner offers, or to schedule regular scans when they do not interfere with your work.

Contents

- On-demand scanning methods and how they are defined
- How scanning of remote storage works
- How scan deferral works
- How heuristic network check for suspicious files works
- How system utilization works
- Configuring on-demand scan tasks

On-demand scanning methods and how they are defined

The on-demand scanner uses these two methods of scanning:

In memory process scanning

This method examines all active processes prior to running the on-demand scan task. A detected potentially unwanted process is highlighted and the process is stopped. This means that a single pass with the on-demand scanner removes all instances of a potentially unwanted program.

Incremental or resumable scanning

This method allows the scanner to start where it last left off. For a scan where you scheduled a start and stop time or a time limit, the scan stops when the time limit is reached. On the next scheduled scan, the on-demand scan continues from the point in the file and folder structure where the previous scan stopped.

How scanning of remote storage works

Remote storage data storage is hierarchical, with two defined levels.:

- The upper level, local storage, includes the NTFS disk volumes of the computer running Remote Storage on Windows 2000 Server.

- The lower level, remote storage, is located on the robotic tape library or stand-alone tape drive that is connected to the server computer.

Remote Storage automatically copies eligible files on your local volumes to a tape library, then monitors space available on the local volumes. File data is cached locally so that it can be accessed quickly as needed. When necessary, Remote Storage moves data from the local storage to remote storage. When you need to access a file on a volume managed by Remote Storage, open the file as usual. If the data for the file is no longer cached on your local volume, Remote Storage recalls the data from a tape library.

How scan deferral works

To improve performance, you can defer on-demand scan tasks when battery power is low or during presentations. You can also allow the user to defer scheduled scans for one-hour increments between one and twenty four hours or to defer it forever. Each user deferral is one hour in duration. For example, if the **Defer at most** option is set at 2, the user can defer the scan task two times or two hours. When the maximum specified number of hours elapses, the scan continues. If the administrator allows unlimited deferrals by setting the option to zero, the user can continue deferring the scan forever.

How heuristic network check for suspicious files works

This feature provides customers using Windows-based McAfee anti-virus products with the most up-to-date real-time detections for certain malware. It uses administrator-configured sensitivity levels to look for suspicious programs and DLLs running on client systems that are protected by VirusScan Enterprise. When the real-time malware defense detects a suspicious program, it sends a DNS request containing a fingerprint of the suspicious file to a central database server hosted by McAfee Avert Labs. The real-time defense feature does not provide protection for entire classes of malware; just for suspicious samples. The benefit of protecting against specific threats is our capability to protect users with McAfee security at virtually the same time that McAfee Avert Labs determines a sample is malicious. In this release, the feature is disabled by default. You must select a sensitivity level to enable the feature.

How system utilization works

System utilization is determined when an on-demand scan starts. CPU and IO samples are taken over the first 30 seconds, then the scan is performed based on the utilization level you specified.

The system utilization you specify does not apply to encrypted files. The decryption is done by LSASS.EXE, not by the Scan32 process. Scanning encrypted files is CPU intensive, therefore even if the system limit on the scanning thread is low, it is still scanning files fast enough that LSASS.EXE must keep busy to supply the decrypted data.

Configuring on-demand scan tasks

VirusScan Enterprise includes a default on-demand scan task. You can use the default task and/or create new tasks.

To access the on-demand scan task:

- From the ePolicy Orchestrator console, go to **Systems | System tree | Client Task**. Select an existing on-demand task or to access the default task, click **New Task**, then from the **Type** list, select **On-Demand Scan (VirusScan Enterprise 8.7.0)** and click **Next**.
- From the VirusScan Console, select an existing on-demand scan task, or to access the default task, open the **Full Scan** properties. If you installed the AntiSpyware Enterprise Module, open the **Targeted Scan** properties. To create a new task, select **Task | New On-Demand Scan Task**.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Scan Locations	• Specify which locations and items to scan. • Include subfolders when scanning. • Include boot sectors when scanning.
Scan Items	• Configure which files and file types to scan. • Enable on-demand scanning for unwanted programs. • Scan inside archives and decode MIME encoded files. • Scan files that have been backed up to storage. • Scan for potential threats that resemble unwanted programs, Trojan horses, and macro viruses.
Exclusions	Configure which disks, files, and folders to exclude from scanning.
Performance	• Configure when to defer scans and for how long. • Specify the system utilization percentage. • Configure the sensitivity level for heuristic network check for suspicious files.
Actions	For threat detections: • Primary action to take when a threat is detected. • Secondary action to take on a threat detection if the first action fails. For unwanted program detections: • Primary action to take when an unwanted program is detected. • Secondary action to take on an unwanted program detection if the first action fails. For allowed actions in the prompt dialog box, select the action.
Reports	• Enable activity logging. • Specify the log file name and location. • Specify the log file size limit. • Select the log file format. • Specify what to log besides scanning activity. • If you installed the AntiSpyware Enterprise Module, alert when cookies are detected.

Tab	Description
Task	Specify where the on-demand scan task runs. NOTE: This tab is only available via ePolicy Orchestrator.

Scanning Email On-Delivery and On-Demand

The email scanner automatically examines email messages and attachments:

- For Microsoft Outlook, email is scanned on delivery or you can invoke on-demand email scans directly from Microsoft Outlook.
- For Lotus Notes, email is scanned when accessed.

Contents

- How heuristic network check for suspicious files works
- Configuring email scan properties

How heuristic network check for suspicious files works

This feature provides customers using Windows-based McAfee anti-virus products with the most up-to-date real-time detections for certain malware. It uses administrator-configured sensitivity levels to look for suspicious programs and DLLs running on client systems that are protected by VirusScan Enterprise. When the real-time malware defense detects a suspicious program, it sends a DNS request containing a fingerprint of the suspicious file to a central database server hosted by McAfee Avert Labs. The real-time defense feature does not provide protection for entire classes of malware; just for suspicious samples. The benefit of protecting against specific threats is our capability to protect users with McAfee security at virtually the same time that McAfee Avert Labs determines a sample is malicious. In this release, the feature is disabled by default. You must select a sensitivity level to enable the feature.

Configuring email scan properties

To access the **On-Delivery Email Scan** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **On-Delivery Email Scanner Policies** in the **Category** list.
- From the VirusScan Console, open the **On-Delivery Email Scanner** properties.

To access the **On-Demand Email Scan** properties:

- From Microsoft Outlook, select **Tools | E-mail Scan Properties**.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Scan Items	• Specify which messages and attachments to scan. • Scan for potential threats that resemble malware. • Scan for unknown macro viruses. • Find attachments with multiple extensions. • Scan inside archives and decode MIME encoded files. • Enable the email scanner to scan for unwanted programs. • Scan email message bodies. • Configure the sensitivity level for heuristic network check for suspicious files. NOTE: This option is available only for **On-Delivery Email Scanning**.
Actions	For threat detections: • Primary action to take when a threat is detected. • Secondary action to take if the first action fails. For unwanted program detections: • Primary action to take when an unwanted program is detected. • Secondary action to take if the first action fails. For allowed actions in the prompt dialog box, select the action.
Alerts	• Notify another user when a threatened email message is detected. • Specify the message that displays to the user when prompting for action.
Reports	• Enable activity logging. • Specify the log file name and location. • Specify the log file size limit. • Select the log file format. • Specify what to log besides scanning activity.
Notes Scanner Settings	NOTE: This tab is available only for **On-Delivery Email Scanning**. Configure Lotus Notes specific settings. • Scan all server databases. • Scan server mailboxes in the specified mailbox root folder. • Notes applications to ignore.

Defining the Quarantine Policy

Detected files, registry keys, and registry values are quarantined based on the quarantine policy you configured. You can restore quarantined items as necessary.

Contents

- Configuring the quarantine policy and restoring items

Configuring the quarantine policy and restoring items

To access the **Quarantine** policy and **Restore** properties, refer to each method described below.

Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

ePolicy Orchestrator — Quarantine Policy

From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **Quarantine Manager Policies** in the **Category** list.

Tab descriptions

Tab	Description
Policy	• Specify the quarantine location • Configure the length of time to keep the quarantined items.

ePolicy Orchestrator — Restore from Quarantine Task

From the ePolicy Orchestrator console, go to **Systems | System Tree | Client Tasks** and select **New Task**, then under **Type** select **Restore from Quarantine (VirusScan Enterprise 8.7.0)**.

Tab descriptions

Tab	Description
Restore	Specify which items to restore. NOTE: The name of the item to restore can be found in the log file as the detection name.
Task	Specify the user account that can access the quarantine location.

VirusScan Console — Quarantine Manager Policy

From the VirusScan Console, open the **Quarantine Manager Policy** properties.

Tab descriptions

Tab	Description
Quarantine	• Specify the quarantine location. • Configure the length of time to keep the quarantined items.
Manager	• Restore, rescan, delete, and view quarantined items. NOTE: The name of the item to restore can be found in the log file as the detection name. • Check quarantined items for false positives.

Configuring Alerts and Notifications

Being notified when a potential threat is detected is an important part of protecting your environment. You can use Alert Manager or VirusScan Enterprise local alerting to notify you when detections occur.

- Alert Manager is a discrete component that works with VirusScan Enterprise to handle alerts and events in real time. In a typical configuration, Alert Manager resides on a central server and listens for alerts sent to it by VirusScan Enterprise. Use it to configure where and how alerts are sent and what the alert message is.
- VirusScan Enterprise provides an interface for configuring Alert Manager and other alerting options that do not require Alert Manager. Filter alerts by severity to limit alert traffic sent to Alert Manager and configure local alerting options that do not require Alert Manager.

Contents

▸ Configuring alerts

Configuring alerts

To access the **Alerts** properties:

- From the ePolicy Orchestrator console, go to **Systems | Policy Catalog** and select **VirusScan Enterprise 8.7.0** in the **Product** list and **Alerts Policies** in the **Category** list.
- From the VirusScan Console, select **Tools | Alerts**.

  Configure the options on each tab. For option descriptions, click **?** or **Help** on each tab.

Tab descriptions

Tab	Description
Alert Manager Alerts	• Specify which components generate alerts. • Configure Alert Manager.
Additional Alerting Options	• Filter alerts by severity. • Configure local alerting.

Accessing Queries and Dashboards

Use queries and dashboards to monitor activity and help you determine what action to take on detections. You can use the predefined queries and dashboards and create additional ones to meet you needs. For information about queries and dashboards, see the ePolicy Orchestrator product documentation.

Queries

To access queries in the ePolicy Orchestrator console, go to **Reporting**, then under **Queries**, scroll down to queries starting with **VSE**.

These predefined queries are available:

- VSE: Compliance Over the Last 30 Days
- VSE: Computers with Threats Detected per Week
- VSE: Current DAT Adoption
- VSE: DAT Adoption Over the Last 24 Hours
- VSE: DAT Deployment
- VSE: Detection Response Summary
- VSE: Number of Detections by Tag
- VSE: Spyware Detected in the Last 24 Hours
- VSE: Spyware Detected in the Last 7 Days
- VSE: Summary of Threats Detected in the Last 24 Hours
- VSE: Summary of Threats Detected in the Last 7 Days
- VSE: Threat Count by Severity
- VSE: Threat Names Detected per Week
- VSE: Threats Detected in the Last 24 Hours
- VSE: Threats Detected in the Last 7 Days
- VSE: Threats Detected Over the Previous 2 Quarters
- VSE: Threats Detected per Week
- VSE: Top 10 Access Protection Rules Broken
- VSE: Top 10 Buffer Overflows Detected
- VSE: Top 10 Computers with the Most Detections
- VSE: Top 10 Detected Threats
- VSE: Top 10 Threat Sources
- VSE: Top 10 Threats per Threat Category
- VSE: Top 10 Users with the Most Detections
- VSE: Unwanted Programs Detected in the Last 24 Hours
- VSE: Unwanted Programs Detected in the Last 7 Days
- VSE: Version 8.5 Compliance
- VSE: Version 8.7 Compliance

Dashboards

To access dashboards in the ePolicy Orchestrator console, go to **Dashboards**

These predefined dashboards are available:

- VSE: Trending Data
- VSE: Current Detections

Responding to Detections

There are different ways to take action on detections depending on which feature detects the threat.

Contents

- How actions are taken on detections
- System access point violations
- Buffer overflow detections
- Unwanted program detections
- On-access scan detections
- On-demand scan detections
- Email scan detections
- Quarantined items

How actions are taken on detections

When a detection occurs, the resulting action depends on how the detection definition is defined in the DAT file. For example, if the scanner cannot clean a file or if the file has been damaged beyond repair, the scanner might delete the file or take the secondary action, depending on how it was defined in the DAT file.

When the scanner denies access to files with potential threats, it also appends the filename with an .mcm extension, when the file is saved.

System access point violations

When a system access point is violated, the action taken depends on how the rule was configured:

- If the rule was configured to report, information is recorded in the log file.
- If the rule was configured to block, then the access is blocked.

Review the log file to determine which system access points were violated and which rules detected the violations, then configure the access protection rules to allow users access to legitimate items and prevent users from accessing protected items.

Use these scenarios to decide which action to take as a response.

Detection Type	Scenarios
Unwanted processes	• If the rule reported the violation in the log file but did not block the violation, select the **Block** option for the rule.

Detection Type	Scenarios
	• If the rule blocked the violation but did not report the violation in the log file, select the **Report** option for the rule. • If the rule blocked the violation and reported it in the log file, no action is necessary. • If you find an unwanted process that was not detected, edit the rule to include it.
Legitimate processes	• If the rule reported the violation in the log file but did not block the violation, deselect the **Report** option for the rule. • If the rule blocked the violation and reported it in the log file, edit the rule to exclude the legitimate process.

Buffer overflow detections

When a buffer overflow detection occurs:

- The scanner blocks the detection.
- A message is recorded in the **On-Access Scan Messages** dialog box. View the dialog box, then decide whether to take any of these additional actions:
  - Remove the message — Select the item in the list, then click **Remove**.
  - Create an exclusion — If the detected process is one that you legitimately use or a false positive, create an exclusion using the information in the **On-Access Scan Messages** dialog box. Review the information in the **Name** column to determine the name of the process that owns the writable memory that is making the call. Use the process name to create an exclusion.
  - Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs.

Unwanted program detections

The on-access, on-demand, and email scanners detect unwanted programs based on the **Unwanted Programs Policy** you configured. When a detection occurs, the scanner that detected the potentially unwanted program applies the action that you configured on the **Actions** tab for that scanner.

Review the information in the log file, then decide whether to take any of these additional actions:

- Fine-tune scanning items to make your scans more efficient.
- If a legitimate program was detected, you can exclude it from detection.
- If an unwanted program was not detected, you can add it to the user-defined detection list.
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs.

On-access scan detections

When a detection occurs:

- The scanner takes action according to how you configured the **On-Access Scan Properties**, **Actions** tab.
- A message is recorded in the **On-Access Scan Messages** dialog box.

Review the information in the activity log and/or the **On-Access Scan Messages** dialog box, then decide whether to take any of these additional actions.

- Fine-tune scanning items to make scanning more efficient.
- **On-Access Scan Messages** dialog box — Right-click an item in the list, then select one of these actions:
  - **Clean File** — Attempts to clean the file referenced by the selected message.
  - **Delete File** — Deletes the file referenced by the selected message. The file name is recorded in the log so that you can restore it from the Quarantine Manager.
  - **Select All (ctrl+a)** — Selects all messages in the list.
  - **Remove Message from List (ctrl+d)** — Removes the selected message from the list. Messages that have been removed from the list are still visible in the log file.
  - **Remove All Messages** — Removes all message from the list. Messages that have been removed from the list are still visible in the log file.
  - **Open On-Access Scanner Log File** — Opens the on-access scanner activity log file. This option is available only from the File menu.
  - **Open Access Protection Log File** — Opens the access protection activity log file. This option is available only from the File menu.
  - If an action is not available for the current message, the corresponding icon, button, and menu items are disabled. For example, **Clean** is not available if the file has already been deleted, or **Delete** is not available if the administrator has suppressed the action.
  - **Clean File** — A file cannot be cleaned if the DAT file has no cleaner or it has been damaged beyond repair. If the file cannot be cleaned, the scanner appends an .mcm extension to the file name and denies access to it. An entry is recorded in the log file. In this case, we recommend that you delete the file and restore it from a clean backup copy.
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs.

On-demand scan detections

When a detection occurs, the scanner takes action according to how you configured the **On-Demand Scan Properties**, **Actions** tab.

Review the information in the log file, then decide whether to take any of these additional actions:

- Fine-tune scanning items to make your scans more efficient.
- If you configured the scanner to **Prompt for action**, select the action from the On-Demand Scan Progress dialog box.

- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs.

Email scan detections

When a detection occurs, the scanner takes action according to how you configured the **On-Delivery Email Scan Properties** or **On-Demand Email Scan Properties**, **Actions** tab.

Review the information in the log file, then decide whether to take any of these additional actions:

- Fine-tune scanning items to make your scans more efficient.
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs.

Quarantined items

Review the items in the quarantine directory, then decide whether to take any of these additional actions:

- Restore.
- Rescan.
- Delete.
- Check for false positive.
- View detection properties.

From the ePolicy Orchestrator console, use the **Restore from Quarantine** client task to take action on quarantined items.

From the VirusScan Enterprise Console, use the **Quarantine Manager Policy** options on the **Manager** tab to take actions on quarantined items.

Supplemental Information

Refer to these topics for supplemental information about using VirusScan Enterprise.

Contents

- Accessing user interface options
- Adding and excluding scan items
- Scheduling tasks
- Configuring command-line options
- Connecting to remote systems
- Submitting threat samples for analysis
- Accessing the Avert Labs Threat Library
- Troubleshooting

Accessing user interface options

There are a number of ways to access the standalone version of the VirusScan Enterprise user interface. This information does not apply when using ePolicy Orchestrator to manage the product.

VirusScan Console and how it works

The VirusScan Console is the interface for the standalone version of the program's activities. Use either of these methods to open the VirusScan Console:

- From the **Start** menu, select **Programs | McAfee | VirusScan Console**.
- Right-click the VirusScan Enterprise shield icon in the system tray, then select **VirusScan Console**.

The VirusScan Console is separated into these sections:

- **Menu bar** -— Use the menu items to create tasks, configure properties, and access additional information.
  - **Task** — Create and configure tasks such as scanning for threats or updating the DAT files.
  - **Edit** — Copy, paste, delete, or rename the selected task.
  - **View** — Display the Toolbar and/or Status bar and refresh the display.
  - **Tools** — Configure interface options for users, lock or unlock user interface security, configure alerts, access the event viewer, open a remote console if you have administrator rights, import or edit the repository list, and roll back the DAT files.

- **Help** — Access online Help topics, the Threat Library on the Avert Labs website, the Submit a Sample website, and the Technical Support website. You can also repair the product installation and view the **About** dialog box for copyright information and which versions of the product, license, definition files, scanning engine, extra driver, and patch are installed.

  NOTE: Each item on the menu has an associated shortcut key. The shortcut key is underlined for each item. These shortcut keys might not be available on some operating systems unless you use the keyboard (F10 or ALT) to access the menus.

- **Toolbar** — Use the icons to access these commonly used commands:
  - Display properties of the selected task.
  - Start the selected task.
  - Stop the selected task.
  - Copy the selected task.
  - Paste the selected task.
  - Delete the selected task.
  - Configure alerting properties.
  - Launch the event viewer.
  - Access the Information Library on the Avert Labs website.
  - Connect to a remote computer if you have administrator rights.
  - Create a new on-demand scan.
- **Task list** — Displays the default tasks and any new tasks that you create as well as the status and last result for each task.
- **Status bar** — Displays the status of the current activity.

Using right-click features

Use right-click features for quick access to commonly used actions such as creating new tasks, viewing task statistics and logs, opening task property pages, scanning a specific file or folder, or performing an immediate update task.

Feature descriptions

Location	Description	Examples
The console	Right-click the VirusScan Console to display right-click features. These features vary depending on whether you selected a task in the task list and which task you select.	• In the console, right-click a task to access its properties. Depending on which task you select, you might also be able to start, stop, enable or disable it, and view statistics and the activity log. In some cases, you can also rename or delete a task. • Right-click a blank area in the console to create a new scan or update task.
Windows Explorer	Right-click a selected file or folder to perform an immediate **Full Scan** of that item. You can select an action for the scan: • **Clean** - Report and clean the detected item. • **Continue** - Report the detection and continue scanning.	Perform an immediate scan on a file or folder that you suspect is threatened. When you start the scan, the on-demand scanner is invoked directly with all scan settings enabled. Select the action option.

Location	Description	Examples
		You cannot customize any other scan settings.
The system tray	Right-click the VirusScan Enterprise shield icon to display menu items.	• Open the VirusScan Console. • Disable or enable the on-access scanner. • Open the on-access scanner properties. • View the on-access scan statistics or messages. • Create a one-time configurable on-demand scan. • Perform an immediate update task. • Open the **About** dialog box.

System tray icon and how it works

Once VirusScan Enterprise is installed, the shield icon appears in the Windows system tray if you configured this feature during the installation process.

Note the following:

- The icon changes when the on-access scanner detects access protection violations. A red frame surrounds the icon for 30 minutes unless you reset it. For more information, see *Access violations and how VirusScan Enterprise responds* in the *Protecting Your System Access Points* section.
- Double-click the icon to display these menu options:
  - **VirusScan Console** — Opens the VirusScan Console.
  - **Disable On-Access Scan** — Toggles between disable and enable.

    NOTE: The access protection, buffer overflow protection, and script scan features use the on-access scanner. If the on-access scanner is disabled, you are not protected from access violations, buffer overflows, or execution of unwanted scripts.

  - **On-Access Scan Properties** — Opens the on-access scanner property pages.
  - **On-Access Scan Statistics** — Displays on-access scanner statistics from which you can enable or disable the on-access scanner and open the on-access scanner property pages.
  - **On-Access Scan Messages** — Displays the on-access scanner messages, where you can take action on items in the list.
  - **On-Demand Scan** — Opens the on-demand scan task property pages for an unsaved task, where you create a one-time on-demand scan task.
  - **Update Now** — Performs an immediate AutoUpdate task.
  - **About VirusScan Enterprise** — Displays information about the product, license, and which version(s) of the scan engine, detection definition files, extra driver (extra.dat), and patches are installed.

Start menu and how it works with VirusScan Enterprise

From the Windows **Start** menu, select **Programs | McAfee** to access these menu items:

- **VirusScan Console** -— Opens the VirusScan Console.

- **On-Access Scan** — Opens the on-access scan property pages.
- **On-Demand Scan** -— Opens the on-demand scan property pages where you configure and perform a one-time unsaved **Full Scan**.

Command line and using it to configure VirusScan Enterprise

Use the command line to perform activities from the Command Prompt. See *Command-line Options* for more information.

Adding and excluding scan items

When configuring detection settings, each of the VirusScan Enterprise scanners allows you to fine-tune the list of file types scanned.

Specifying scan items

Fine-tune your scanning capabilities by adding scan items to the default list or by creating a specific list of extensions to scan.

Option definitions

Option	Definition
File types to scan	• **Default + additional file types** — Specify additional file extensions and whether to also scan for macros in all files. The maximum number of additional file type extensions that the scanner can accommodate is 1,000. • **Specified file types only** — Create a list of specific extensions to scan. The maximum number of additional file type extensions that the scanner can accommodate is 1,000.

Specifying exclusions

Specify files, folders, and drives to exclude from scanning operations. You can also remove any exclusions you specified previously.

Option definitions

Option	Definition
What not to scan	Select the type of exclusion. • **Exclude by pattern —** Specify the pattern(s) and whether to include subfolders. • **Exclude by file type —** Specify a file type(s). • **Exclude by file age —** Specify the access type and minimum age in days. • **Protected by Windows File Protection —** Exclude files that have Windows Protection File status.

Using wildcards to specify scan items

When using wildcards to specify or exclude scan items, these limitations apply:

- Valid wildcards are question mark (?) for excluding single characters and asterisk (*) for excluding multiple characters.
- Wildcards can appear in front of a back slash (\) in a path. For example: C:\ABC*\XYZ matches C:\ABC\DEF\XYZ.
- An exclusion containing question mark (?) characters applies if the number of characters matches the length of the file or folder name. For example: The exclusion W?? excludes WWW, but does not exclude WW or WWWW.
- The syntax is extended to include a double asterisk (**), which means *zero or more of any characters including back slash*. This allows multiple-depth exclusions. For example: C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\DEF\DEF\XYZ, etc.

Scheduling tasks

You have the option to schedule on-demand, AutoUpdate, and mirror tasks to run at specific dates and times, or intervals.

Configuring the task schedule

Configure the task to run at a specified time or interval.

NOTE: You must have administrator rights to schedule the task. Administrator rights provide the user with write access to the scheduled task's registry key.

To schedule a task, click the **Schedule** button in the task's properties dialog box.

Tab descriptions

Tab	Description
Task	• Enable scheduled task to run at specified times. • Stop the task if it runs for the specified hours and minutes. • Specify user account settings; user name, domain, and password.
Schedule	Specify the schedule frequency and associated settings.

Configuring command-line options

You can install, configure, and run VirusScan Enterprise from the command line. Installation options are described in the VirusScan Enterprise Installation Guide. This section describes options for performing on-demand scanning and update tasks.

Configuring on-demand scanning command-line options

The on-demand scanner uses *SCAN32.EXE* to detect threats.

The *SCAN32* syntax does not require any specific order on its elements, except that you cannot separate a property and its value. This syntax consists of:

- **File name** — The name of the executable file: *SCAN32.EXE*.
- **Options** — The option is preceded by a forward slash (/) character and is not case-sensitive.

For example, SCAN32 PROPERTY=VALUE [,VALUE] [/option].

On-demand scanning option definitions

Command-line Option	Definition
ALL	Scans all files in the target folder.
ALLOLE	Scans default files plus all Microsoft Office documents.
ALWAYSEXIT	Forces exit from on-demand scan, even if scan completed with error/failure.
APPLYNVP	Scans for the potentially unwanted programs that are defined in the Unwanted Programs Policy.
ARCHIVE	Scans archive files such as .ZIP, .CAP. LZH, and .UUE files.
AUTOEXIT	Exits the on-demand scanner upon completion of a non-interactive scan.
CLEAN	Cleans the detected target file when a potentially unwanted program is found.
CLEANA	Cleans the detected file when an unwanted program is found.
CONTINUE	Continues scanning after a potentially unwanted program is detected.
CONTINUE2	Continues scanning after a potentially unwanted program is detected and the primary action has failed.
CONTINUEA	Continues scanning after an unwanted program is detected.
CONTINUEA2	Continues scanning after an unwanted program is detected and the primary action has failed.
DEFEXT	Adds file extensions that you specify as parameters to the list of selected file types that are included in scanning.
DELETE	Deletes the detected file when a potentially unwanted program is found.
DELETE2	Deletes the detected file when a potentially unwanted program is found and the primary action has failed.
DELETEA	Deletes the file when an unwanted program is detected.
DELETEA2	Deletes the file when a potentially unwanted program is detected and the primary action has failed.
EDIT	Displays the scan properties dialog box.
EXT	Replaces the extensions on the list of selected file types that are included in scanning with the file extensions that you add, as parameters following this argument.
LOG	Logs detection reports to a previously specified log file.
LOGFORMAT <value>	Uses the specified format for the log file. Valid values are ANSI, UTF8, or UTF16.
LOGSETTINGS	Logs the configuration settings of a scan.
LOGSUMMARY	Logs a summary of scan results.
LOGUSER	Logs identifying information about the user who executes a scan.
MHEUR	Enables heuristic detection of macro threats.
MIME	Detects potentially unwanted programs in mime (Multipurpose Internet Mail Extensions) encoded files.
NOESTIMATE	Does not calculate scan size before beginning scanning of files. Progress bar does not display.
PHEUR	Enables heuristic detection of non-macro threats.

Command-line Option	Definition
PRIORITY	Sets the priority of the scan relative to other CPU processes. Requires an additional numerical parameter. A value of 1 assigns priority to all other CPU processes. A value of 5 assigns the highest priority to the scan.
PROMPT	Prompts the user for action when a potentially unwanted program is detected.
PROMPT2	Prompts the user for action when a potentially unwanted program is detected and the primary action has failed.
PROMPTA	Prompts the user for action when an unwanted program is detected.
PROMPTA	Prompts the user for action when an unwanted program is detected.
PROMPTA	Prompts the user for action when an unwanted program is detected.
PROMPTA	Prompts the user for action when an unwanted program is detected.
PROMPTA2	Prompts the user for action when an unwanted program is detected and the primary action has failed.
RPTSIZE	Sets the size of the alert log, in Megabytes.
START	Runs the scan. Does not display the properties dialog box.
TASK	Launches the on-demand scanner task specified in the VirusScan Console. Requires additional parameter specifying the specified task ID as recorded in the registry at: hkey_local_machine_\software\McAfee\Desktop\Protection\Tasks.
UINONE	Launches the scanner without making the user interface dialog visible.

Configuring update task command-line options

VirusScan Enterprise uses *MCUPDATE.EXE* to perform update tasks.

The *MCUPDATE* syntax does not require any specific order in its elements, except that you cannot separate a property and its value. The syntax consists of:

- **File name** — The name of the executable file: *MCUPDATE.EXE*.
- **Options** — The option is preceded by a forward slash (/) character and is not case-sensitive.

For example, MCUPDATE [/<type> [/TASK <guid>]] [/option].

The /TASK clause is optional. If you use it however, you must also specify an update task ID (guid). The task ID you select must be for an update or a rollback DATs task. Do not select to scan ID. If you do not specify a task ID, the default update task is used. Task IDs are located at: hkey_local_machine\SOFTWARE\McAfee\DesktopProtection\Tasks\

The /OPTION clause is not required. To perform a silent update task, use /QUIET.

NOTE: The /QUIET option is not supported for use with the rollback DATs task. This example performs a silent update task: MCUPDATE [/UPDATE] [/QUIET].

Update task option definitions

Command-line Option	Definition
ROLLBACKDATS	Rolls the current DAT file back to the last backed up version.
UPDATE	Performs an update of the DAT file, scanning engine, product, or extra.dat.
/TASK	Launches the AutoUpdate or rollback DATs task specified in the VirusScan Console. Requires an additional parameter to specify the task ID as recorded in the registry at:

Command-line Option	Definition
	hkey_local_machine\software\McAfee\DesktopProtection\Tasks
/QUIET	Performs the task silently.

Connecting to remote systems

You can connect to remote systems with VirusScan Enterprise installed to perform operations such a modifying or scheduling scanning or update tasks, or enabling and disabling the on-access scanner on a remote system.

NOTE: If you do not have administrator rights to connect to the remote system, you receive an *Insufficient user rights access denied* message.

When you start the **VirusScan Remote Console**, the name of the system you are connected to appears in the console title bar. If you have not connected to a system elsewhere on the network, the title bar does not show the name of your local system. When you open any task's properties dialog box from a remote console, the system name is displayed in the properties dialog box title bar.

You can open multiple remote consoles. When you close the **Connect to Remote Computer** dialog box, the connection to the remote system closes as well.

Accessing remote systems with VirusScan Enterprise installed

To connect to remote systems with VirusScan Enterprise installed.

Task

From the VirusScan Console **Tools** menu, select **Open Remote Console**.

1 Under **Connect to computer**, type the name of the system that you want to administer, and select a system from the list, or click **Browse** to locate the system on the network.

   NOTE: If environmental variables are used while configuring the path name of the file or folder for a remote task, be sure that the environmental variable exists on the remote system. The VirusScan Console cannot validate environmental variables on the remote system.

2 Click **OK** to make a connection attempt to the destination system.
When you connect to the remote system:

   - The title bar changes to reflect that system's name.
   - The console reads the remote system's registry and displays the tasks of the remote system. You can add, delete, or reconfigure tasks for the remote system.

Submitting threat samples for analysis

If you find a potential threat that is not being detected with the current DAT file, you can submit a sample of it to McAfee Avert Labs through WebImmune. They analyze the sample and consider it for inclusion in the DAT file.

If the scanner detects something that you think it should not detect, you can also submit a sample of it to Avert Labs through WebImmune. Avert analyzes it and considers excluding it from the DAT file.

You can submit a sample to Avert Labs through WebImmune by directly accessing the web site, via email, or via standard mail.

WebImmune

From the VirusScan Console, select **Help | Submit a Sample** to access the website.

The website is located at: https://www.webimmune.net/default.asp.

1. Log on to your free account, or create one.
2. Upload files directly to the Avert Labs automated systems for review. Items are escalated to the Avert Labs analysts if additional research is required.

Email

Send emails directly to the Avert Labs automated systems for review. Items are escalated to the Avert Labs analysts if additional research is required.

The global email address is virus_research@avertlabs.com.

NOTE: Get additional regional addresses from the WebImmune website.

Standard Mail

Get the address from the WebImmune website.

NOTE: This is the least preferred method and causes the longest turnaround time for review of your sample.

Accessing the Avert Labs Threat Library

To access the Avert Labs Threat Library from the VirusScan Console, select **McAfee Avert Labs Threat Library** from the **Help** menu.

Troubleshooting

This section contains troubleshooting information for the VirusScan Enterprise product.

Repairing the product installation

Use the VirusScan Enterprise repair installation utility to restore the program's default installation settings and/or reinstall all of the program files.

To access the **Repair Installation** utility, from the VirusScan Console, select **Help | Repair Installation**.

NOTE: This feature is not available from the ePolicy Orchestrator console.

Option definitions

Option	Definition
Restore all settings to installation defaults	Restores the VirusScan Enterprise default installation settings. CAUTION: Customized settings might be lost.
Reinstall all program files	Reinstalls the VirusScan Enterprise program files. CAUTION: Hotfixes, Patches, and/or Service Packs might be overwritten.

Frequently asked questions

This section contains troubleshooting information in the form of frequently asked questions.

Installation

- **Question:** I just installed the software using the silent installation method, and there is no VirusScan Enterprise icon in the Windows system tray.

  Answer: The icon shield does not appear in the system tray until you restart your system. However, even though there is no icon, VirusScan Enterprise is running and your system is protected. Verify this by checking for the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ ShStatEXE="C:\Program Files\McAfee\VirusScan Enterprise\SHSTAT.EXE"/STANDALONE.

- **Question:** Why can some users on my network configure their own settings and others cannot?

  Answer: The administrator might have configured the user interface so that tasks are password-protected. If so, users cannot change settings. In addition, different Windows operating systems have different user privileges. Refer to your Microsoft Windows documentation for more information about user privileges.

Potentially unwanted programs

- **Question:** I suspect I have a potentially unwanted program but VirusScan Enterprise is not detecting it.

  Answer: Download the latest beta DAT file while it is still being tested prior to the official release, from this website: http://vil.nai.com/vil/virus-4d.asp.

Blocked programs

- **Question:** I installed VirusScan Enterprise and now one of my programs does not work.

  Answer: The program might be blocked by an access protection rule.

  1. Review the access protection log file to determine if the program was blocked by a rule.
  2. If you find the program listed in the log, you can either enter it as an exclusion to the rule or disable the rule. See *Protecting Your System Access Points* for more information.

Cookie detections

- **Question:** When reviewing the cookie detections in the on-demand scan activity log, I noticed that the file name detection is always *00000000.ie* for every detection. Why does

VirusScan Enterprise assign the same file name for every on-demand scan cookie detection when other programs assign an individual or incremental file name to each cookie detection?

Answer: VirusScan Enterprise assigns the same file name to each cookie detection because of the way the on-demand scanner detects and takes action on cookies. This behavior applies only to cookies detected by on-demand scans. A cookie file might contain many cookies. The scan engine treats a cookie file as an archive and assigns a value as an offset from the beginning of the file (starting with zero). Because the scanner uses the scan engine to detect and take action on each detected cookie before it proceeds with the scan, the value starts at zero for each detection. The result is that every detection is assigned a 00000000.ie file name. Other products detect all cookies, assign each one an individual or incremental file name, then take action on each detection.

General

- **Question:** The VirusScan Enterprise icon in my system tray appears to be disabled.

  Answer: If there is a red circle and line covering the VirusScan Enterprise icon, that indicates that the on-access scanner is disabled. Here are the most common causes and solutions. If none of these solves your problem, contact Technical Support.

  1. Make sure that the on-access scanner is enabled. Right-click the VirusScan Enterprise icon in the system tray. If the on-access scanner is disabled, click **Enable On-Access Scan**.
  2. Make sure that the McShield service is running.
     - Start the service manually from the Services Control Panel.
     - Select **Start | Run**, then type **Net Start McShield**.
     - Set the service to start automatically from the Services Control Panel.

- **Question:** I get an error saying that I cannot download *CATALOG.Z*.

  Answer: This error can be caused by many things. Here are some suggestions to help determine the source of the problem:

  - If you are using the McAfee default download site for updates, determine if you can download the *CATALOG.Z* file from a web browser. Try downloading the file from this website: http://update.nai.com/Products/CommonUpdater/catalog.z.
  - If you can't download the file, but you can see it (in other words, your browser does not allow you to download it), you have a proxy issue and need to talk to your network administrator.
  - If you can download the file, VirusScan Enterprise should be able to download it as well. Contact technical support for assistance in troubleshooting your installation of VirusScan Enterprise.

- **Question:** What is the location of the HTTP download site?

  Answer:

  - The McAfee download site location is: http://www.mcafeesecurity.com/us/downloads/updates/default.asp.
  - The *CATALOG.Z* file, which contains the latest updates, can be downloaded from this website: http://update.nai.com/Products/CommonUpdater/catalog.z.

- **Question:** What is the location of the FTP download site?

  Answer:

  - The FTP download site location is: ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x.

  - The *CATALOG.Z* file, which contains the latest updates, can be downloaded from this site: ftp://ftp.mcafee.com/CommonUpdater/catalog.z.

- **Question:** If I do detect a potentially unwanted program and I have chosen **prompt user for action**, what action should I choose (**Clean** or **Delete**)?

  Answer: Our general recommendation is to choose **Clean** if you are not sure what to do with a detected file. The on-access and on-demand scanners automatically back up items to the quarantine directory before they are cleaned or deleted.

Index

A

access protection 6, 13, 14, 15, 16, 17, 18, 45
- about 6
- access violations 14
- anti-virus and common rules 16
- common rules 13
- detections and actions 45
- excluding processes 18
- file/folder blocking rules 17
- getting started 13
- port blocking rules 16
- preconfigured rules 13
- protocols, restricting 15
- registry blocking rules 17
- removing unused rules 18
- standard and maximum protection 14
- types of rules 14
- user-defined rules 14, 15, 16
- virtual machine protection 14

access protection, configuring 15
actions
- unwanted programs 46

Actions tab, VirusScan Enterprise 37
actions, VirusScan Enterprise
- access protection 45
- access violations 14
- buffer overflow detections 46
- email scanning 48
- on-access scanning 45, 47
- on-demand scanning 37, 47
- quarantined items 48
- responding to a threat 44

activity logs
- unwanted programs 46

activity logs, VirusScan Enterprise
- access violations 14
- buffer overflow reports 19
- email scanning and 39, 48
- on-access scanning 33
- on-demand scanning and 37, 47
- reviewing 47

adware (See unwanted programs) 21
Alert Manager
- access violations 14
- configuring alerts 43
- events 15

alerts, VirusScan Enterprise
- about 6
- configuring 43
- email scanning 39
- on-demand scanning 37
- overview 43

anti-virus rules
- configuring access protection 16

anti-virus rules *(continued)*
- preconfigured access protection 13

AutoUpdate
- process overview 24
- repositories, connecting to 25
- strategies for VSE updates 23

B

bandwidth
- updating strategies and 23

best practices
- removing EXTRA.DAT files from repositories 25
- strategies for VSE updates 23
- updating DAT files and engine 8

Blocking tab, VirusScan Enterprise 33
buffer overflow protection
- about 6
- configuring 19
- detections and actions 46
- exploits, overview 19

C

CATALOG.Z file, encrypted update 24
command line, using it to configure the product 52
common rules
- access protection, configuring 16
- preconfigured access protection 13
- standard and maximum protection 14

configuring process settings 33
CPU usage
- risk assignment and Windows Task Manager 31

D

dashboards
- monitoring activity 44
- predefined, accessing 44

DAT file updating
- getting started 8
- strategies 23
- update tasks, about 24

DAT files
- detection definitions 23
- detections and defined actions 45
- EXTRA.DAT files, updating 24
- scheduling rollouts 23
- script scanning and 30

deployment
- scheduling VSE update tasks 23

detection definitions (See DAT files) 23
detections
- access protection 45
- actions in response to 45
- buffer overflow 46
- configuring general settings 33

detections *(continued)*
email scanning 39, 48
on-access scanning 47
on-demand scanning 37, 47
responding to 44
dialers (See unwanted programs) 21
documentation
product 9
release notes 10

E

email scanning
about 6
configuring 39
detections and actions 48
engine updating
AutoUpdate, process overview 24
getting started 8
strategies 23
events, VirusScan Enterprise
access violations 14
Alert Manager 15
exclusions
identifying processes for 46
on-demand scanning 37
using wildcards to specify scan items 52
what not to scan 52
Exclusions tab, VirusScan Enterprise 37
extension files
VirusScan Enterprise 8

F

false positives
creating exclusions to reduce 46
file type extensions
what not to scan 52
what to scan 52
files and folders
blocking, configuring access protection 17
restricting access 15

G

General tab, VirusScan Enterprise 32

H

heuristic scanning 33
high-risk processes
assigning risk 31
configuring VirusScan Enterprise 32
settings 32

L

log files
access protection, configuring 15
log files, VirusScan Enterprise
access violations 14
buffer overflow reports 19
email scanning and 39
on-access scanning 33
on-demand scanning and 37
low-risk processes
assigning risk 31
configuring VirusScan Enterprise 32
low-risk processes *(continued)*
settings 32

M

Messages tab, VirusScan Enterprise 33

N

notifications, VirusScan Enterprise
about 6
configuring 43
overview 43

O

on-access scanning
about 6
assigning risk to a process 31
deciding how many scanning policies 31
detections and actions 45, 47
general and process settings 32
overview 29
process settings 33
reading from vs. writing to disk 30
risk assignment 31
scanning policies 31
script scanning 30
on-delivery email scanning (See email scanning) 6
on-demand scanning
about 6
configuring tasks 37
detections and actions 47
exclusions 37
incremental, resumable, in-memory 35
methods 35
remote storage scans 35
scan deferral 36
system utilization 36

P

passwords
controlling access to VSE interface 11
protecting phone book files 13
User Interface Options policy 11
performance
Windows Performance Monitor 31
Performance tab, VirusScan Enterprise 37
policies
unwanted Programs 46
policies, VirusScan Enterprise
Alert Policies 43
email scanning 39
on-access scanning 31
On-Delivery Email Scan Policies 39
Quarantine Manager 41
unwanted programs 21
User Interface Options 11
ports
access protection, configuring 16
blocking network traffic on 14, 15
potentially unwanted programs (See unwanted programs) 21
process settings 33
processes
settings, on-access scanning 33
processes, VirusScan Enterprise
assigning risk to 31

processes, VirusScan Enterprise *(continued)*
default, configuring 32
in memory process scanning 35
incremental or resumable scanning 35
low-risk and high-risk 32
script scanning 30

Q

quarantines, VirusScan Enterprise
about 6
configuring 41
detections and actions 48
restore tasks, configuring 41
queries, VirusScan Enterprise
about 6
accessing from ePO navigation bar, Reporting 44
monitoring activity 44
predefined, list of 44

R

registry keys
access protection, configuring 17
restricting access 15
reports
accessing queries 44
configuring VSE logging 39
on-access scanning activity 33
on-demand scanning activity 37
Reports tab, VirusScan Enterprise 33, 37
repositories
AutoUpdate, connecting to 25
central, using for VSE updates 23
removing EXTRA.DAT files from 25
rules, VirusScan Enterprise
anti-virus 16
file/folder blocking 17
port-blocking 16
registry blocking 17
removing unused 18
user-defined, types of 15

S

Scan Items tab, VirusScan Enterprise 22, 37
Scan Locations tab, VirusScan Enterprise 37
scanning
activity logs 46
adding and excluding scan items 52
assigning risk to a process 31
email scans (See email scanning) 39
exclusions, specifying 52
file type extensions, specifying 52
heuristic 33
on-access (See on-access scanning) 29
on-demand (See on-demand scanning) 35
using wildcards to specify scan items 52
script scanning (See on-access scanning) 30
ScriptScan tab, VirusScan Enterprise 33
settings, VirusScan Enterprise
general and process, defined 32
general, configuring 32
spyware (See unwanted programs) 21
system tray icon
access violations and 14
configuring access to VSE interface 11

T

task
mirror 26
update 24
task, scheduling 53
Tasks tab, VirusScan Enterprise 38
threat detections (See threats) 39
threats
access violations 45
buffer overflow 46
email scanning 48
on-access detections and actions 45
on-access scanning 47
on-demand scanning 47
quarantined items 48
responding to 44
unwanted programs 46
tuning, VirusScan Enterprise
what to scan, adding and excluding 52

U

unwanted programs
about VSE protection 6
actions and on-demand scanning 37
configuring policy for 21
detections and actions 46
email scanning, actions 39
on-demand scanning 35
overview 21
updating, VirusScan Enterprise
AutoUpdate 24
extension files 8
process overview 24
strategies 23
tasks 23
update sites 25
update task 6, 23
user accounts
access to quarantined items, configuring 41
access to VSE interface, controlling 11
user interface security
about 6
configuring 11
passwords and 11
User-Defined Items tab, VirusScan Enterprise 22
user-defined rules, access protection 14

V

virtual machine protection rules
preconfigured access protection 14
VirusScan Enterprise
access protection 13, 14
buffer overflow protection 19
email scanning 39
features, described 6
general settings, configuring 32
getting started 8
notifications and alerts 43
on-access scanning 29, 47
on-demand scanning 35
quarantine policy 41
removing unused rules 18
Restore From Quarantine task 41, 48
unwanted programs policy 21
updating 23, 24

VirusScan Enterprise *(continued)*
user interface security 11
what to scan, adding and excluding 52

W

wildcards, using in scan items 52
Windows
Explorer, risk assignment and 32
File Protection, exclusions 52
Task Manager, assigning risk 31